

**DETAILED ACTION**

***Response to Arguments***

1. Applicant's arguments with respect to claims 1-34 have been considered but are moot in view of the new ground(s) of rejection.

***Response to Amendment***

2. The Examiner has stated the below column and line numbers as examples. All columns and line numbers in the reference and the figures are relevant material and Applicant should be taken the entire reference into consideration upon the reply to this Office Action.
3. Claims 1, 7, 12, 16 and 33 have been amended.
4. Claims 2, 8 and 31 have been cancelled.
5. Claim 34 has been added.
6. Claims 1, 3-7, 9-30 and 32-34 are pending.

***Information Disclosure Statement***

7. No Information Disclosure Statements have been submitted by the Applicant.

***Drawings***

8. In light of Applicant's amendments, the previous objection to the drawings has been withdrawn.

***Claim Objections***

9. Claims 9, 27 and 29 objected to because of the following informalities: the status of each claim is that of Currently Amended, but there is no indication of any amendment. The Examiner assumes that this is a typographical error and the claim status is Previously Presented. Appropriate correction is required.

***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

12. Claims 1, 3-7, 9-30 and 32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication No. 2003/0140151 to Daenen et al. (hereinafter Daenen) in view of US Patent No. 7,073,055 to Freed et al. (hereinafter Freed).

As to claims 1 and 33, Daenen teaches:

- a. Receiving authentication messages sent through an access server from a user to an authentication server (user logs in through the access server to the connection policy server to the authentication server) (Daenen, [0040-0041]).
- b. Determining from said authentication messages user identifiers and service attributes associated with said user (message information is used to build a profile for the user that specifies the rules governing network access of the user) (Daenen, [0043-0045]).
- c. Creating a user service policy entry in a user policy table, in a network device separate from the access server and the authentication server (the Connection Policy RADIUS Server (CPRS) is separate and independent of the access server and authentication server) (Daenen, [0032 and 0051]) for said identified user contained said service attributes

(message information is used to build a profile for the user that specifies the rules governing network access of the user) (Daenen, [0043-0045]).

Daenen teaches that the CPRS can be used to monitor user accesses which are distinguished from access requests, but does not expressly mention managing user traffic subsequent to authentication (Daenen, [0015]). However, in an analogous art, Freed teaches:

d. Consulting said user policy table to determine how to manage said user traffic directed to a service-providing server and sent subsequent to said user authentication messages (policy profile of a user defines filters that are used to manage user's access to specific resources after user authentication) (Freed, col. 14, lines 4-30).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the access control of Daenen with the policy profile of a user that manages the user's access to the requested resource in order differentiate between normal and premium server users as suggested by Freed (Freed, col. 14, lines 18-56).

Daenen as modified further teaches:

e. Managing subsequent user traffic based on said consulting step (policy server keeps user profile which is used to determine the execution of rules governing user access) (Daenen, [0015]).

As to claim 3, Daenen as modified teaches said user policy table is located within said service policy director (storage module stores profile of user and is part of CPRS) (Daenen, [0047-0049]).

As to claims 4, 10 and 14, Daenen as modified teaches said service policy director offers internal network services comprising at least one of bandwidth management (user profile attributes include access-rate settings) (Freed, column 14, lines 21-23).

As to claims 5, 9 and 13, Daenen as modified teaches said authentication messages are using the RADIUS protocol (RADIUS) (Daenen, [0038]).

As to claims 6, 11 and 15, Daenen as modified teaches proxy mode, wherein the authentication messages in a provider network pass through the service policy director, said network device modifies IP addresses of said authentication messages without any modification to the data of said authentication messages (CPRS can act as a proxy to the other servers) (Daenen, [0051]).

As to claims 7 and 34, Daenen as modified teaches:

- a. Determining by the service policy director a user policy table based on an at least an initial authentication message sent from a user to an authentication server using an access server (log in information is used to

build a profile for the user that specifies the rules governing network access of the user) (Daenen, [0043-0045]).

b. Identifying a user originating said network user traffic (CPRS constructs a profile of the user during authentication process) (Daenen, [0041 and 0043-0044]).

c. Consulting the user policy table to locate a user service policy corresponding to said user (policy server keeps user profile which is used to determine the execution of rules governing user access) (Daenen, [0015 and 0044]), (policy profile of a user defines filters that are used to manage user's access to specific resources after user authentication) (Freed, col. 14, lines 4-30).

d. Managing said network user traffic based on said consulting step by forwarding network user traffic to a requested server (filter rules are applied to input and output queues and direct traffic to the requested network services) (Freed, col. 14, lines 4-40).

As to claim 12, Daenen as modified teaches:

a. Receiving authentication messages for a user from an access server at said service policy director (user logs in through the access server to the connection policy server to the authentication server) (Daenen, [0040-0041]).

b. Determining user identities and service attributes associated with said user from at least a first authentication message from an

authentication server (message information is used to build a profile for the user that specifies the rules governing network access of the user) (Daenen, [0043-0045]).

c. Creating a user service policy entry in a user policy table for said identified user based on said service attributes (message information is used to build a profile for the user that specifies the rules governing network access of the user) (Daenen, [0043-0045]).

d. Consulting said user policy table to determine how to manage said user traffic directed to a service-providing server sent subsequent to said user authentication messages (policy server keeps user profile which is used to determine the execution of rules governing user access) (Daenen, [0015 and 0044]) and (Daenen, [0015 and 0044]), (policy profile of a user defines filters that are used to manage user's access to specific resources after user authentication) (Freed, col. 14, lines 4-30).

e. Managing subsequent user traffic based on said consulting step (filter rules are applied to input and output queues and direct traffic to the requested network services) (Freed, col. 14, lines 4-40).

As to claim 16, Daenen as modified teaches:

a. A user request-issuing device (client computer) (Daenen, [0037] and fig. 1, ref. 17).

- b. An access server forwarding authentication messages and user traffic from and to the user request-issuing device (access server) (Daenen, [0037] and fig. 1, ref. 12).
- c. A service provider network over which user authentication messages and user traffic directed to service-providing server, both of which originated from said user request-issuing device is transmitted (network) (Daenen, [0037]).
- d. An authentication server to which said user request-issuing device attempts to connect and by which said user request-issuing device is authenticated and registered (AAA) (Daenen, [0037] and fig. 1, ref. 15).
- e. A network device independent of said authentication server including a service policy director enforcing a service policy for said user request-issuing device, said network device receiving the authentication messages and creating the service policy therefrom (the Connection Policy RADIUS Server (CPRS) is separate and independent of the access server and authentication server) (Daenen, [0032 and 0051]).
- d. Said service policy director enforcing said service policy on user requests directed to service-providing servers subsequent to the authentication and registration (policy profile of a user defines filters that are used to manage user's access to specific resources after user authentication) (Freed, col. 14, lines 4-30).

As to claim 17, Daenen as modified teaches said service policy director includes a user policy table (storage module stores profile of user and is part of CPRS) (Daenen, [0047-0049]).

As to claim 18, Daenen as modified teaches said policy table includes user identifier information and service attribute information (storage module stores profile of user which includes user specific information and policy rules that apply to the specific user) (Daenen, [0047-0050]).

As to claim 19, Daenen as modified teaches said user identifier information includes at least an Internet/intranet address (IP address is part of user profile) (Freed, column 13, line 60-column 14, line 7).

As to claim 20, Daenen as modified teaches said user identifier information a username (user profile contains user identity which can include a username) (Freed, column 13, lines 18-47).

As to claim 21, Daenen as modified teaches said attribute information includes any one or more of the following: access privileges parameters, traffic logging mechanisms and user activity statistics entitlement parameters, security services entitlement parameters, or service quality level parameters (service parameters are specified in the user profile) (Freed, column 18, lines 10-42).

As to claim 22, Daenen as modified teaches said service quality level parameters include any one or more of the following: a bandwidth limit, a bandwidth guarantee, or a bandwidth priority (maximum bandwidth is defined) (Freed, column 19, lines 1-3).

As to claim 23, Daenen as modified teaches said service attributes define services offered by said service policy director, said services including any one or more of the following: classification of network user traffic, modification of network user traffic, forwarding of network user traffic, or logging of single network user traffic statistics (at least two types of network service: normal service type and premium service type) (Freed, column 17, lines 40-63 and figures 7A and 7B).

As to claim 24, Daenen as modified teaches said network device offers internal network services including at least one of bandwidth management, access control or network usage statistics (network entities have an internal bandwidth manager) (Freed, column 8, lines 5-18).

As to claim 25, Daenen as modified teaches a plurality of said service policy directors reside on a network (network is composed of a plurality of operational, administrative and maintenance servers) (Freed, column 7, lines 23-52).

As to claim 26, Daenen teaches said network device including said service policy director functioning in a transparent mode, wherein the authentication messages in a provider network pass through the network device without any modification to the IP addresses and data of said authentication messages (the CPRS is transparent to the BAS and AAA) (Daenen, [0041]).

As to claim 27, Daenen teaches said service policy director functioning in said transparent mode receives said user authentication request messages addressed to said authentication server and forwards said user authentication request messages to said authentication server (the CPRS is transparent to the BAS and AAA) (Daenen, [0041]).

As to claim 28, Daenen teaches said network device including said network device including said service policy director functioning in a proxy mode, wherein the authentication messages in a provider network pass through the network device, said network device modifies IP addresses of said authentication messages without any modification to the data of said authentication messages (server acts as a proxy to other information servers) (Daenen, [0051]).

As to claim 29, Daenen teaches said service policy director functioning in said proxy mode receives said user authentication messages addressed to said service policy director and forwards it to said authentication server (server acts as a proxy to other information servers) (Daenen, [0041 and 0051]).

As to claim 30, Daenen as modified teaches said network device comprising said service policy director functioning in a passive mode, wherein the authentication messages in a provider network are copied to the network device (a first network device creates the certificates and these certificates are transferred to RADIUS server for authentication) (Freed, column 18, lines 10-42).

As to claim 32, Daenen as modified teaches said service policy director functions in a transparent mode, wherein the authentication messages in a provider network pass through the service policy director without any modification to the IP address and data of said authentication messages (the CPRS is transparent to the BAS and AAA) (Daenen, [0041]).

### ***Conclusion***

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will

Art Unit: 2434

the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to WILLIAM S. POWERS whose telephone number is (571)272-8573. The examiner can normally be reached on m-f 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/W. S. P./  
Examiner, Art Unit 2434

William S. Powers  
Examiner  
Art Unit 2434

3/26/2009

/Andrew L Nalven/  
Primary Examiner, Art Unit 2434